CLAIMS

1. A method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) transmitting a first communication from a first network device to a second network device, wherein the first communication includes a challenge;

(B) in response to receiving the challenge, generating a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge;

(C) transmitting a second communication from the second network device to the first network device, the second communication including the preliminary hash value; and

(D) completing performance of the hash function on the first network device to produce a final hash value.

2. The method of claim 1, wherein act (B) comprises:

performing only part of a Message Digest 5-based encryption function.

3. The method of claim 2, wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and wherein act (B) comprises:

(1) generating an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device; and

(2) inputting the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

4. The method of claim 1, wherein the complete performance of the hash function involves performing a first number of iterations, act (B) includes performing a second number of iterations less than the first number of iterations and act (D) includes performing a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function.

5. The method of claim 1, wherein act (D) includes completing the hash function using a second part of the challenge, wherein the first part and the second part form the complete challenge.

6. The method of claim 1, wherein act (B) includes generating the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

7. The method of claim 6, wherein act (B) includes dividing the challenge into the first part and a second part, and the method further comprises:

(E) configuring the second communication to include an indication of a length in bits of the user credential, and

wherein act (D) includes completing the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

8. The method of claim 7, wherein act (D) includes:

(1) determining a state of the hash function based, at least in part, on the length of the user credential; and

(2) completing the hash function based, at least in part, on the determined state.

9. The method of claim 7, wherein act (D) further comprises:

(1) determining a length of the second part based, at least in part, on a length of the challenge and the length of the user credential; and

(2) completing the hash function based, at least in part, on the determined length of the second part.

10. The method of claim 1, further comprising an act of:

(E) generating the challenge on the first network device, including generating a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and appending bits to the portion of the challenge to produce the challenge.

11. The method of claim 10, wherein act (E) includes appending sixty-three bits to the portion.

12. The method of claim 1, wherein the challenge includes a plurality of sequences of bits, the method further comprising an act of:

(E) generating the challenge on the first network device, including configuring one or more of the plurality of sequences to include at least one non-zero bit.

13. The method of claim 12, wherein each sequence is an octet of bits.

14. The method of claim 1, further comprising an act of:

(E) generating the challenge on the first network device, including configuring the challenge to include at least a minimum number of octets of bits.

15. The method of claim 1, wherein act (B) comprises:

(1) determining a length of a concatenation of an authentication protocol identifier, a user credential and the challenge; and

(2) dividing the challenge into the first part and a second part based on the determined length.

16. The method of claim 1, further comprising an act of:

(E) authenticating the user based on the final hash value.

17. The method of claim 1, wherein the method further comprises an act of:

(E) transmitting a third communication including the final hash value to a third network device configured to authenticate the user.

18. The method of claim 1, wherein act (A) includes transmitting the first communication within a tunnel between the first network device and the second network device and Act (C) includes transmitting the second communication within the tunnel.

19. A system for at least partially authenticating a user on a communications network, the system comprising:

a first communication device operative to transmit a first communication from a first network device to a second network device, wherein the first communication includes a challenge; and

a second network device, operative to receive the challenge, generate a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge, and to transmit a second communication from the second network device to the first network device, the second communication including the preliminary hash value,

wherein the first network device is operative to complete performance of the hash function to produce a final hash value.

20. The system f claim 19, wherein the second network device is operative to perform only part of a Message Digest 5-based encryption function.

21. The system of claim 20, wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and

wherein the second network device is operative to generate an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device, and to input the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

22. The system of claim 19, wherein the complete performance of the hash function involves performing a first number of iterations, and the second network device is operative to perform a second number of iterations less than the first number of iterations, and wherein the first network device is operative to perform a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function.

23. The system of claim 19, wherein the first network device is operative to complete the hash function using a second part of the challenge, wherein the first part and the second part form the complete challenge.

24. The system of claim 19, wherein the first network device is operative to generate the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

25. The system of claim 24, wherein the second network device is operative to divide the challenge into the first part and a second part, and to configure the second communication to include an indication of a length in bits of the user credential, and the first network device is operative to complete the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

26. The system of claim 25, wherein the first network device is operative to determine a state of the hash function based, at least in part, on the length of the user credential, and to complete the hash function based, at least in part, on the determined length.

27. The system of claim 25, wherein the first network device is operative to determine a length of the second part based, at least in part, on a length of the challenge and the length of the user credential, and to complete the hash function based, at least in part, on the determined length of the second part.

28. The system of claim 19, wherein the first network device is operative to generate the challenge on the first network device, including generating a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and to append bits to the portion of the challenge to produce the challenge.

29. The method of claim 28, wherein the first network device is operative to append sixty-three bits to the portion.

30. The system of claim 19, wherein the challenge includes a plurality of sequences of bits, and the first network device is operative to generate the challenge on the first network device, including configuring one or more of the plurality of sequences to include at least one non-zero bit.

31. The system of claim 30, wherein each sequence is an octet of bits.

32. The system of claim 19, wherein the first network device is operative to generate the challenge on the first network device, including configuring the challenge to include at least a minimum length of bits.

33. The system of claim 19, wherein the second network device is operative to determine a length of a concatenation of an authentication protocol identifier, a user credential and the challenge, and to divide the challenge into the first part and a second part based on the determined length.

34. The system of claim 19, wherein the first network device is operative to authenticate the user based on the final hash value.

35. The system of claim 19, wherein the first network device is operative to transmit a third communication including the final hash value to a third network device configured to authenticate the user.

36. The system of claim 19, wherein the first network device is operative to transmit the first communication within a tunnel between the first network device and the second network device.

37. The system of claim 19, wherein the second communication device is operative to transmit the second communication with a tunnel between the first device and the second device.

38. A system for at least partially authenticating a user on a communications network, the system comprising:

a first communication device operative to transmit a first communication from a first network device to a second network device, wherein the first communication includes a challenge; and

a second network device operative to receive the challenge and transmit a second communication from the second network device to the first network device, the second communication including a preliminary hash value,

wherein the second network device includes means for generating a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge, and

wherein the first network device includes means for completing performance of the hash function to produce a final hash value.

39. A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by a computer, control the computer to perform a method of at least partially authenticating a user on a communications network, the method comprising:

(A) transmitting a first communication from a first network device to a second network device, wherein the first communication includes a challenge;

(B) in response to receiving the challenge, generating a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge; and

(C) transmitting a second communication from the second network device to the first network device, the second communication including the preliminary hash value; and

(D) completing performance of the hash function on the first network device to produce a final hash value.

40. A method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) transmitting a first communication from a first network device to a second network device, wherein the first communication includes a challenge;

(B) receiving a second communication from the second network device to the first network device, the second communication including a preliminary hash value resulting from

performance of only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge; and

(C) completing performance of the hash function on the first network device to produce a final hash value.

41. The method of claim 40, wherein the preliminary hash value is a result of partial performance of an Message Digest 5-based encryption function on the first part of the challenge, and wherein act (C) comprises:

completing the Message Digest 5-based encryption function.

42. The method of claim 40, wherein the complete performance of the hash function involves performing a first number of iterations, and wherein the preliminary hash value resulted from performance of a second number of iterations less than the first number of iterations, and

wherein act (C) includes performing a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function

43. The method of claim 40, wherein act (C) includes completing the hash function using a second part of the challenge, wherein the first part and the second part form the complete challenge.

44. The method of claim 40, wherein the challenge includes two parts: the first part and a second part, and the preliminary hash value is based, at least in part, on the first part of the challenge and a user credential, and the second communication includes an indication of a length in bits of the user credential, and

wherein act (C) includes completing the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

45. The method of claim 44, wherein act (C) includes:

(1) determining a state of the hash function based, at least in part, on the length of the user credential; and

(2) completing the hash function based, at least in part, on the determined state.

46. The method of claim 44, wherein act (C) further comprises:

(1) determining a length of the second part based, at least in part, on a length of the challenge and the length of the user credential; and

(2) completing the hash function based, at least in part, on the determined length of the second part.

47. The method of claim 40, further comprising an act of:

(D) generating the challenge on the first network device, including generating a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and appending bits to the portion of the challenge to produce the challenge.

48. The method of claim 43, wherein act (D) includes appending sixty-three bits to the challenge.

49. The method of claim 40, wherein the challenge includes a plurality of sequences of bits, the method further comprising an act of:

(D) generating the challenge on the first network device, including configuring one or more of the plurality of sequences to include at least one non-zero bit.

50. The method of claim 49, wherein each sequence is an octet of bits.

51. The method of claim 40, further comprising an act of:

(D) generating the challenge on the first network device, including configuring the challenge to include at least a minimum length of bits.

52. The method of claim 40, further comprising an act of:

(D) authenticating the user based on the final hash value.

53. The method of claim 40, wherein the method further comprises an act of:

(D) transmitting a third communication including the final hash value to a third network device configured to authenticate the user.

54. A tunnel server residing on a first network device of a communications network for at least partially authenticating a user on the communications network, the tunnel server comprising:

a challenge generator to generate a challenge that is transmitted from the first network device to a second network device;

a final hash value generator to receive a preliminary hash value from the second network device, the preliminary hash value resulting from performance of only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge,

wherein the final hash value generator is operative to complete performance of the hash function on the first network device to produce a final hash value.

55. The tunnel server of claim 54, wherein the complete performance of the hash function involves performing a first number of iterations, and the preliminary hash value is the result of performance of a second number of iterations less than the first number of iterations, and wherein the final hash value generator is operative to perform a third number of iterations equal to the first number minus the second number, resulting in a complete performance of the hash function.

56. The tunnel server of claim 54, wherein the final hash value generator is operative to complete the hash function using a second part of the challenge, wherein the first part and the second part form the complete challenge.

57. The tunnel server of claim 54, wherein the challenge includes the first part and a second part, and the second communication includes an indication of a length in bits of a user credential, and

wherein the final hash value generator is operative to complete the hash function based, at least in part, on the second part of the challenge and the length of the user credential.

58. The tunnel server of claim 57, wherein the final hash value generator is operative to determine a state of the hash function based, at least in part, on the length of the user credential, and to for complete the hash function based, at least in part, on the determined length.

59. The tunnel server of claim 57, wherein the final hash value generator is operative to determine a length of the second part based, at least in part, on a length of the challenge and the

length of the user credential, and to complete the hash function based, at least in part, on the determined length of the second part.

60. The tunnel server of claim 54, wherein the challenge generator is operative to generate the challenge, to generate a portion of the challenge having a length equal to a desired amount of entropy for the challenge, and to append bits to the portion of the challenge to produce the challenge.

61. The tunnel server of claim 60, wherein the challenge generator is operative to append sixty-three bits to the portion.

62. The tunnel server of claim 54, wherein the challenge includes a plurality of sequences of bits, and the challenge generator is operative to generate the challenge, and to configure one or more of the plurality of sequences to include at least one non-zero bit.

63. The tunnel server of claim 62, wherein each sequence is an octet of bits.

64. The tunnel server of claim 54, wherein the challenge generator is operative to generate the challenge, including configuring the challenge to include at least a minimum length of bits.

65. The tunnel server of claim 54, wherein the tunnel server is operative to authenticate the user based on the final hash value.

66. The tunnel server of claim 54, wherein the tunnel server is operative to control transmission of a third communication including the final hash value to a third network device configured to authenticate the user.

67. The tunnel server of claim 54, wherein the tunnel server is operative to control transmission of the first communication within a tunnel between the first network device and the second network device.

68. A tunnel server residing on a first network device of a communications network for at least partially authenticating a user on the communications network, the tunnel server comprising:

a challenge generator to generate a challenge that is transmitted from the first network device to a second network device, wherein the tunnel server is operative to receive a preliminary hash value from the second network device, the preliminary hash value resulting from performance of only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge; and

means for completing performance of the hash function on the first network device to produce a final hash value.

69. A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by a computer, control the computer to perform a method of at least partially authenticating a user on a communications network, the method comprising acts of:

(A) transmitting a first communication from a first network device to a second network device, wherein the first communication includes a challenge;

(B) receiving a second communication from the second network device to the first network device, the second communication including a preliminary hash value generated by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge; and

(C) completing performance of the hash function on the first network device to produce a final hash value.

70. A method of at least partially authenticating a user on a communications network in response to a challenge received at a second network device from a first network device, the method comprising acts of:

(A) generating a preliminary hash value by performing only part of a hash function on a first part of the challenge wherein the first part is less than the complete challenge; and

(B) transmitting a communication from the second network device to the first network device, the communication including the preliminary hash value.

71. The method of claim 70, wherein act (A) comprises:

performing only part of a Message Digest 5-based encryption function.

72. The method of claim 71, wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and wherein act (A) comprises:

(1) generating an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device; and

(2) inputting the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

73. The method of claim 70, wherein the complete performance of the hash function involves performing a first number of iterations, and act (A) includes performing a second number of iterations less than the first number of iterations.

74. The method of claim 70, wherein act (A) includes generating the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

75. The method of claim 74, wherein act (A) includes dividing the challenge into the first part and a second part, and the method further comprises:

(E) configuring the communication to include an indication of a length in bits of the user credential.

76. The method of claim 70, wherein act (A) comprises:

(1) determining a length of a concatenation of an authentication protocol identifier, a user credential and the challenge; and

(2) dividing the challenge into the first part and a second part based on the determined length.

77. The method of claim 70, wherein act (A) includes transmitting the first communication within a tunnel between the first network device and the second network device..

78. A client residing on a second network device of a communications network, for at least partially authenticating a user in response to a challenge received on the second network device from a first network device, the client comprising:

a preliminary hash generator to generate a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge,

wherein the second network device is operative to transmit a communication from the second network device to the first network device, the communication including the preliminary hash value.

79. The client of claim 78, wherein the preliminary hash generator is operative to perform only part of a Message Digest 5-based encryption function.

80. The client of claim 79, wherein a standard Message Digest 5 algorithm includes adding an appendage of information to information to be communicated to produce padded information that has a length that is a multiple of sixty-four octets, and includes inputting the padded information to a standard Message Digest 5 function, and

wherein the preliminary hash generator is operative to generate an input sequence to the Message Digest 5-based encryption function by concatenating information to be communicated from the second network device to the first network device, and to input the input sequence into the Message Digest 5-based encryption function without previously adding an appendage of information to the input sequence.

81. The client of claim 78, wherein the complete performance of the hash function involves performing a first number of iterations, and

wherein the preliminary hash generator is operative to perform a second number of iterations less than the first number of iterations.

82. The client of claim 78, wherein the preliminary hash generator is operative to generate the preliminary hash value based, at least in part, on the first part of the challenge and a user credential.

83. The client of claim 82, wherein the preliminary hash generator is operative to divide the challenge into the first part and a second part, and to configure the communication to include an indication of a length in bits of the user credential.

84. The client of claim 78, wherein the preliminary hash generator is operative to determine a length of a concatenation of an authentication protocol identifier, a user credential and the challenge, and to divide the challenge into the first part and a second part based on the determined length.

85. The client of claim 78, wherein the client is operative to control transmission of the first communication within a tunnel between the first network device and the second network device.

86. A client residing on a second network device of a communications network, for at least partially authenticating a user in response to a challenge received on the second network device from a first network device, the client comprising:

means for generating a preliminary hash value by performing only part of a hash function on a first part of the challenge, wherein the first part is less than the complete challenge,

wherein the second network device is operative to transmit a communication from the second network device to the first network device, the communication including the preliminary hash value.

87. A computer-readable medium having computer-readable signals stored thereon that define instructions that, as a result of being executed by a computer, control the computer to perform a method of at least partially authenticating a user on a communications network in response to a challenge received at a second network device from a first network device, the method comprising acts of:

(A) generating a preliminary hash value by performing only part of a hash function on a first part of the challenge wherein the first part is less than the complete challenge; and

(B) transmitting a communication from the second network device to the first network device, the second communication including the preliminary hash value.